

Normal forms of random braids

Volker Gebhardt^{*,†} and Stephen Tawn^{*}

28th February 2013

Abstract

We analyse statistical properties of the normal forms of random braids generated by two different methods, namely generating random words of given length in the generators, respectively generating random braids with uniform distribution on the set of braids of given length.

Except for an initial and a final region whose lengths are uniformly bounded, the distributions of the factors of the normal form of sufficiently long random braids depend neither on the position in the normal form nor on the lengths of the random braids. Moreover, when multiplying a braid on the right, the expected number of factors in its normal form that are modified is uniformly bounded; the latter property yields an algorithm for computing normal forms that has linear expected run time.

1 Introduction

Explicit computations play an increasingly important role in most areas of algebra; the study of braids is no exception. In many situations, computations with braids involve choosing braids at random: Some algorithms explicitly require a random braid to be generated; this is the case, for instance, in cryptographic protocols based on the braid group [AAG99, KLC⁺00]. At other times, a large collection of typical examples is to be generated; this is usually the case in computational experiments supporting theoretical research.

As B_n , the group of braids on n strands, is infinite, choosing braids at random is not a trivial task. There are various natural ways of choosing elements of B_n at random, and different approaches will yield different probability distributions on B_n . For both, computational experiments and applications (especially applications in cryptography), it is important to understand the statistical probabilities of samples of random elements generated using a particular method.

We consider in the following the *braid monoid* B_n^+ defined by the presentation

$$(1) \quad B_n^+ = \left\langle \sigma_1, \dots, \sigma_{n-1} \mid \begin{array}{ll} \sigma_i \sigma_j = \sigma_j \sigma_i & (1 \leq i < j < n) \\ \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1} & (1 \leq i < n-1) \end{array} \right\rangle^+.$$

^{*}Both authors acknowledge support under Australian Research Council's Discovery Projects funding scheme (project number DP1094072).

[†]Volker Gebhardt acknowledges support under the Spanish Project MTM2010-19355.

As the relations of B_n^+ are homogeneous, the number of generators occurring in any expression of $x \in B_n^+$ is well-defined; we call this number the *length* $|x|$ of x . We can then fix a non-negative integer k and generate an element $x \in B_n^+$ of length k . More specifically, there are two possibilities:

- (A) For $i = 1, \dots, k$ independently choose $a_i \in \mathcal{A} = \{\sigma_1, \dots, \sigma_{n-1}\}$ with a uniform probability distribution on \mathcal{A} , or equivalently, consider the set $\mathcal{A}^*|_k$ of all *words* of length k over the alphabet \mathcal{A} , and choose an element of $\mathcal{A}^*|_k$ at random with a uniform probability distribution on this set.
- (B) Consider the set $B_n^+|_k = \{x \in B_n^+ : |x| = k\}$ and choose an element of $B_n^+|_k$ at random with a uniform probability distribution on this set.

We will refer to (A) as *generating uniformly random words*, and to (B) as *generating uniformly random braids*. We will write Word_k , respectively URB_k , for the corresponding probability measures on B_n^+ . Since the number of different words in $\mathcal{A}^*|_k$ that represent the same element x of $B_n^+|_k$ depends on x , generating uniformly random words results in a distribution of *braids* which is very far from being uniform on $B_n^+|_k$. Generating uniformly random braids is not easy; an algorithm whose time-complexity respectively space-complexity is polynomial in both n and k was given in [GGM13].

In this paper we compare the generation of uniformly random braids to the generation of uniformly random words regarding some properties of the generated samples of braids. The *Garside normal form* defines a canonical way of expressing a braid as a sequence of permutations, so a probability distribution on the braid group induces a sequence of probability distributions on the symmetric group. We are particularly interested in how the resulting distributions on the symmetric group depend on the position in this sequence.

The structure of the paper is as follows: section 2 recalls the Garside normal form; experts may skip this section. section 3 contains our analysis of the normal forms of random braids. In subsection 3.1 we show that there is a “stabilisation” occurring in the normal forms of long random braids in the sense that for sufficiently long braids, the distributions on the symmetric group induced by the factors of the normal form depend neither on the position in the normal form nor on the lengths of the random braids, except for an initial and a final region whose lengths are uniformly bounded. In subsection 3.2, we give an explanation for this stabilisation phenomenon by demonstrating that the expected number of factors of the normal form of a braid that are modified when multiplying the braid on the right is uniformly bounded. Finally, in subsection 3.3, we extend our analysis to general Garside groups and establish a criterion for deciding whether the above mentioned phenomena occur in a given Garside group.

2 Background

This section contains a brief summary of the main notions referred to in the paper. Specifically, we will recall Garside monoids and the Garside normal form. For details and proofs we refer to [ECH⁺92, Deh02a].

In a cancellative monoid M with unit $\mathbf{1}$, we can define the *prefix* partial order: For $x, y \in M$, we say $x \preceq y$ if there exists $c \in M$ such that $xc = y$. Similarly, we define the *suffix* partial order by saying that $x \succeq y$ if there exists $c \in M$ such that $x = cy$. We call $s \in M$ an *atom*, if $s = ab$ (with $a, b \in M$) implies $a = \mathbf{1}$ or $b = \mathbf{1}$. We write \mathcal{A} for the set of atoms of M .

A cancellative monoid M is called a *Garside monoid of spherical type*, if it is a lattice (that is, least common multiples and greatest common divisors exist and are unique) with respect to \preceq and with respect to \succeq , if there are no strict infinite descending chains with respect to either \preceq or \succeq , and if there exists an element $\Delta \in M$, such that $D(\Delta) = \{s \in M \mid s \preceq \Delta\} = \{s \in M \mid \Delta \succeq s\}$ is finite and generates M . In this case, we call Δ a *Garside element* and the elements of $D(\Delta)$ the *simple elements* (with respect to Δ). Moreover, we denote the \preceq -gcd and the \preceq -lcm of $x, y \in M$ by $x \wedge y$ respectively $x \vee y$. It follows that, for $s \in D(\Delta)$, there exists a unique element $\partial s \in D(\Delta)$ such that $s \partial s = \Delta$.

We assume for the rest of this section that M is a Garside monoid of spherical type. Since $D(\Delta)$ generates M , every element $x \in M$ can be written in the form $x = x_1 \cdots x_m$ with $x_1, \dots, x_m \in D(\Delta)$. The representation as a product of this form can be made unique by requiring that each simple factor is non-trivial and maximal with respect to \preceq . More precisely, we say that $x = x_1 \cdots x_m$ is in *(left) normal form*, if $x_m \neq \mathbf{1}$ and if $x_i = \Delta \wedge (x_i \cdots x_m)$ for $i = 1, \dots, m$. Equivalently, we can require

$$(2) \quad x_m \neq \mathbf{1} \quad \text{and} \quad \partial x_i \wedge x_{i+1} = \mathbf{1} \quad \text{for } i = 1, \dots, m-1.$$

If a word is in normal form then all occurrences of Δ must be at the start, hence the normal form of x is of the form $\Delta^k x_1 x_2 \cdots x_l$ where $x_i \in D(\Delta) \setminus \{\mathbf{1}, \Delta\}$. We say that $\inf(x) = k$ is the *infimum* of x , $\text{cl}(x) = l$ is the *canonical length* of x , and $\sup(x) = k + l$ is the *supremum* of x .

As M satisfies the Ore conditions, it embeds into its quotient group $Q(M)$. Conjugation by Δ gives a bijection $\tau: D(\Delta) \rightarrow D(\Delta)$ and, as $D(\Delta)$ is finite, this implies that some power of Δ is central. Hence, for every element x of $Q(M)$ there exists an integer k such that $\Delta^k x$ lies in M , and so we can extend the normal form to the quotient group $Q(M)$.

Of particular interest to us in section 3 will be the maps projecting onto the i -th non- Δ factor from the left respectively from the right of the normal form. If $\Delta^k x_1 x_2 \cdots x_l$ is in normal form, we define

$$\lambda_i(x) = \begin{cases} x_i & \text{for } i = 1, 2, \dots, l \\ \mathbf{1} & \text{otherwise} \end{cases} \quad \text{and} \quad \rho_i(x) = \begin{cases} x_{l+1-i} & \text{for } i = 1, 2, \dots, l \\ \mathbf{1} & \text{otherwise} \end{cases}.$$

Classical Garside structure for the braid group

The monoid B_n^+ defined by the presentation (1) is a Garside monoid of spherical type whose quotient group is the braid group B_n on n strands. It is referred to as the *classical Garside monoid* for B_n . The atoms of B_n^+ are the generators $\sigma_1, \dots, \sigma_{n-1}$, and the Garside element Δ of B_n^+ is the so-called *half-twist*, the

positive braid in which any two strands cross exactly once. The simple braids are exactly those braids in which any two strands cross at most once. In particular, a simple braid is characterised by the permutation which it induces on the strands, whence the set $D(\Delta)$ is in bijection to the symmetric group S_n .

Given $x \in B_n^+$, we define the *starting set* of x as $S(x) = \{a \in \mathcal{A} \mid a \preccurlyeq x\}$ and the *finishing set* of x as $F(x) = \{a \in \mathcal{A} \mid x \succcurlyeq a\}$.

We remark that the conditions characterising normal forms can be expressed in terms of strating and finishing sets, as an element $x \in B_n^+$ is simple if and only if it is square-free, that is, if and only if it cannot be written as $x = ua^2v$ with $a, u, v \in B_n^+$ and $a \neq \mathbf{1}$: For any $x \in D(\Delta)$, we have $F(x) \cap S(\partial x) = \emptyset$ and $F(x) \cup S(\partial x) = \mathcal{A}$ [Cha95, Lemma 4.2]. For $u, v \in D(\Delta)$, one therefore has $\partial u \wedge v = \mathbf{1}$ if and only if $S(v) \subseteq \mathcal{A} \setminus S(\partial u) = F(u)$.

3 Normal form

In this section we will investigate the normal form of random elements. For our experiments, we constructed and analysed samples of 9999 elements of B_n^+ for each combination of number of strands $n \in \{5, 10, 15, 20, 25, 30\}$ and word length $k \in \{4, 8, 12, 16, 24, 32, 48, 64, 96, 128, 192, 256, 512, 1024, 2048\}$ for both uniformly random words and uniformly random braids. For uniformly random words we also analysed samples with a word length of 4096. The samples of uniformly random braids were constructed using an implementation of the algorithm described in [GGM13] by the first author; the rest of the computations were done using a development version of MAGMA [BCP97] V2.19.

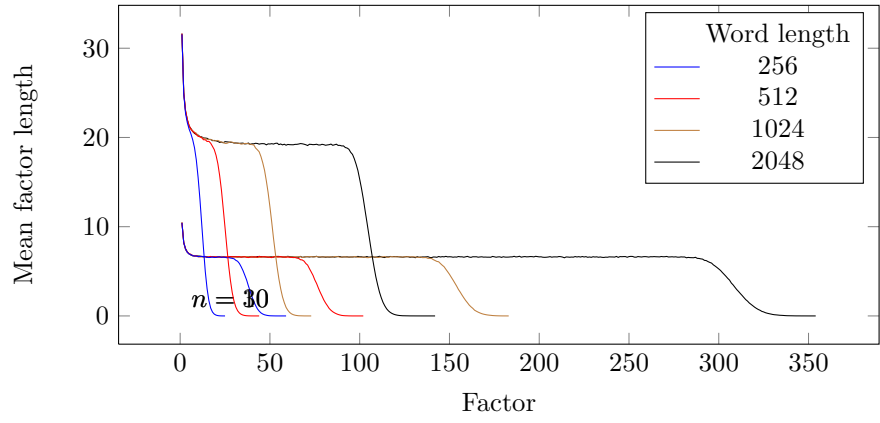
Using these samples we will investigate the distribution of simple factors along the normal form of the elements, that is, we will look at how the induced probability measures $\lambda_{i*}(\text{Word}_k)$, $\lambda_{i*}(\text{URB}_k)$, $\rho_{i*}(\text{Word}_k)$ and $\rho_{i*}(\text{URB}_k)$ on the set of simple elements vary with i . This will lead us to investigate how the normal form changes when an element is multiplied by an atom.

3.1 Stable region

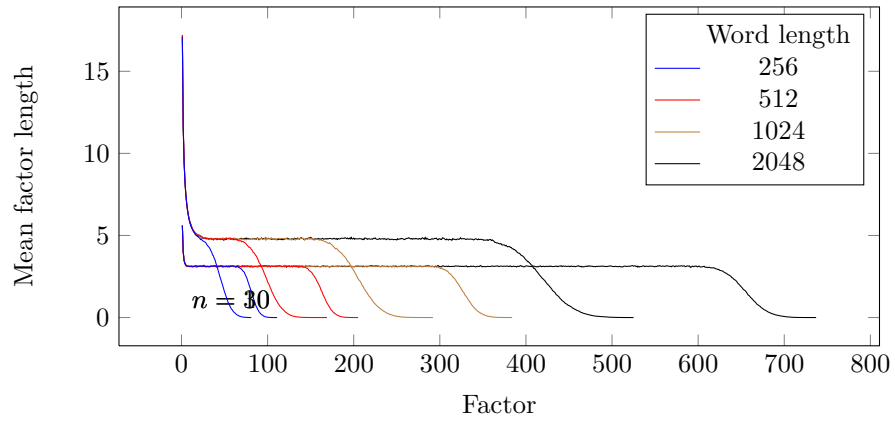
The fact that there are a large number of simple elements makes it impractical to look directly at the distribution at each position of the normal form. So, we will use several invariants instead, namely the word length and the starting and finishing sets, to indirectly probe these distributions.

Word length

Figure 1 shows how the mean factor length varies along the word. We observe that, provided the word is long enough, the word can be divided into three regions: An initial region where the word length of the factors is rapidly decreasing; a stable region where the word length is constant; and a terminal region where it drops to zero. Moreover, the shape and size of this initial region



(a) Uniformly random words



(b) Uniformly random braids

Figure 1: Mean factor length

is independent of the word length. The same structure occurs for the samples not shown here.

The variation in the canonical length within each samples has “smeared out” the terminal region, causing it to grow in size as the word length increases. If we were to draw right justified plots, that is, if the x -axis was the distance from the end, then you would see that, like the initial regions, the terminal regions have a constant size and shape for sufficiently long words.

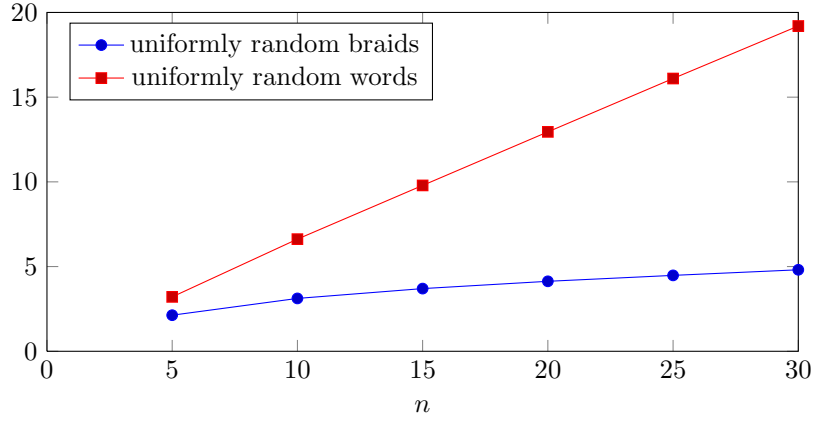


Figure 2: Mean factor length inside stable region.

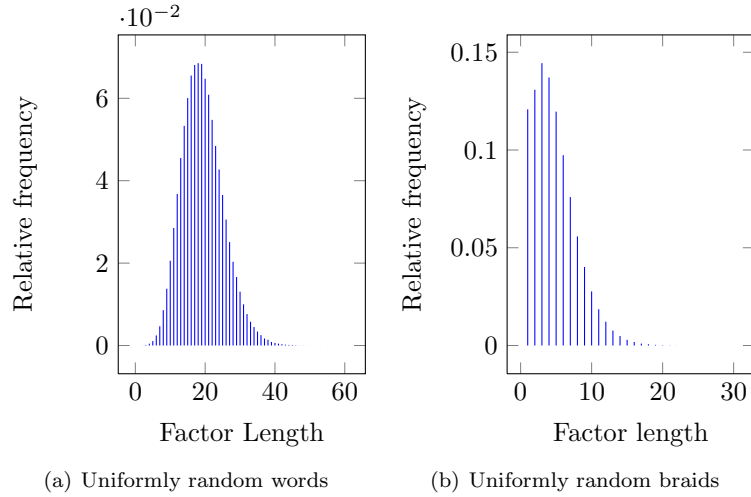


Figure 3: Distribution of factor lengths in the stable region. $n = 30$

Figure 2 shows how the mean factor length inside the stable region depends on n for both uniformly random words and uniformly random braids, and Figure 3 shows the distributions of factor lengths in the stable region for $n = 30$ for both uniformly random words and uniformly random braids.

For uniformly random words, the observed mean factor lengths are consistent with a linear function in n (the best fit of a model of the form n^c is obtained

for $c \approx 0.9952$), whereas for uniformly random braids the mean factor length grows much more slowly; the best fit of a model of the form n^c is obtained for $c \approx 0.44941$.

The data indicates that normal forms of uniformly random words are much more “densely packed” than those of uniformly random braids, and that this difference becomes more pronounced with increasing n . This is consistent with the fact that the distribution of braids obtained by choosing uniformly random words is biased towards multiples of the Garside elements of standard parabolic subgroups, that is, the lcms of subsets of \mathcal{A} [GGM13]. Such lcms have the maximal number representing words, as they can be rewritten using *all* braid relations between the generators involved. On the other hand, these lcms also have the maximal possible word length of all simple elements in the standard parabolic subgroups, that is, they yield the densest possible packing of the involved generators into simple factors.

Starting and finishing sets

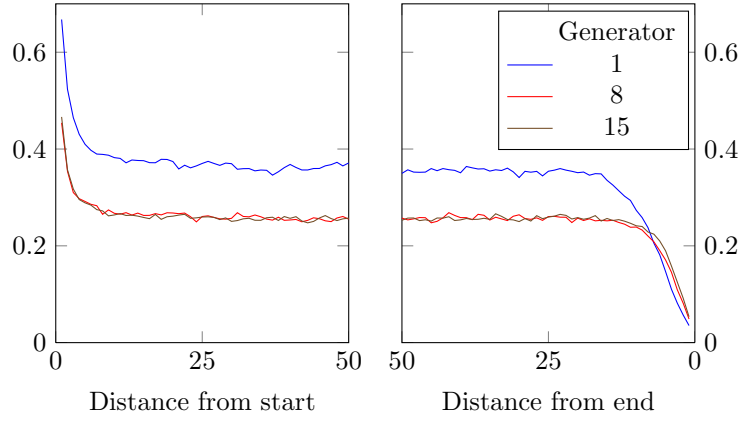
Figure 4 shows, for a given generator, the relative frequency with which that generator lies in the starting set for each canonical factor. To avoid the problem with the variation in canonical length smearing out the end of the words we have drawn a left justified plot for the beginning and a right justified plot for the end of the word. The plots not shown here for different values of n , different word lengths, different generators and for the finishing sets all have a similar shape. As we saw for the mean factor length, there is an initial region, a stable region and a terminal region. In Figure 4 for uniformly random braids and generator 15 there is a local minimum around the 10th factor. Nevertheless, the size and shape of the initial, and terminal, regions remains fixed once the word length is sufficiently long. Furthermore, the sizes of these regions are consistent with the sizes observed for the mean factor length.

One clear difference between uniformly random words and uniformly random braids is in the structure of the starting and finishing sets, see Figure 5. For uniformly random words the distribution is mostly flat only rising at the edges of the braids, whereas for uniformly random braids we have a continuously changing distribution which rises from almost zero at the edges of the braid and peaks in the middle.

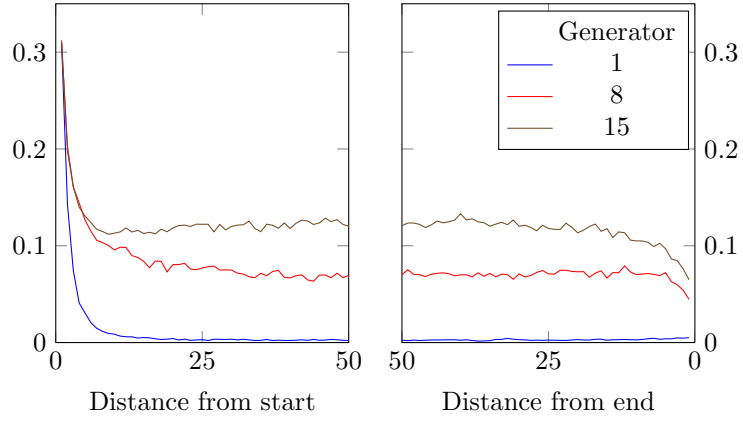
Combining mean word length and starting / finishing set frequencies

Given a sample of random braids, we consider the mean factor length and the relative frequency of each generator being in the starting set respectively in the finishing set as functions f of the position p in the non- Δ factors of the normal form.

For each of these functions f , we identify the interval $[p_1, p_2]$ that minimises the ratio $\frac{|f([p_1, p_2])|}{|[p_1, p_2]|}$, where, for $S \subseteq \mathbb{R}$, we define $|S| = \max(S) - \min(S)$. (Intuitively, this procedure locates the “most horizontal part” of the graph of f .) We then fit a linear model \tilde{f} to $f|_{[p_1, p_2]}$ and accept the interval $[p_1, p_2]$ as stable region for



(a) Uniformly random words



(b) Uniformly random braids

Figure 4: Relative frequency of a generator being in the starting set. $n = 30$, word length = 2048.

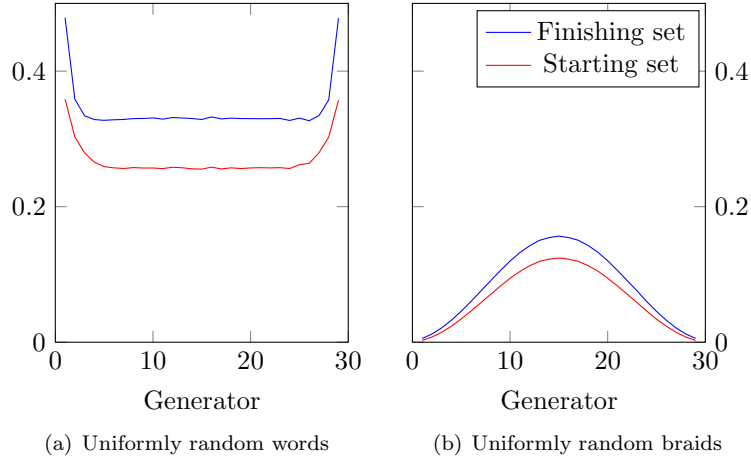


Figure 5: Relative frequency of a generator being in the starting and finishing set in the stable region. $n = 30$

f if $|\tilde{f}([p_1, p_2])| < 0.1 \cdot |f([p_1, p_2])|$; otherwise we consider the stable region for f as empty. (Intuitively, this procedure ensures that the trend in the restriction of f to the interval $[p_1, p_2]$ is small compared to the statistical fluctuations of f on the interval.)

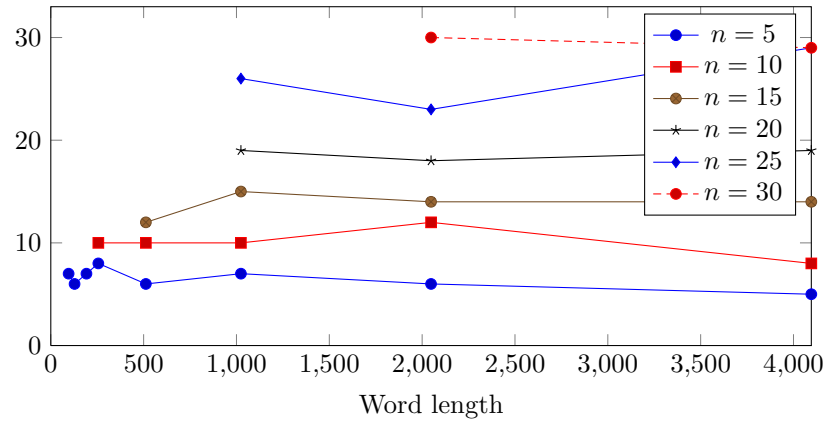
The stable region of the sample is taken to be the intersection of the stable regions for all the functions.

Figure 6 shows the start of the stable region, determined as described above, as a function of n and the word length for both uniformly random words and uniformly random braids. The data shows that, for fixed n and a given method of generating random braids, stable regions exist for sufficiently long random braids, and that their starting position does not depend on the word length of the random braids.

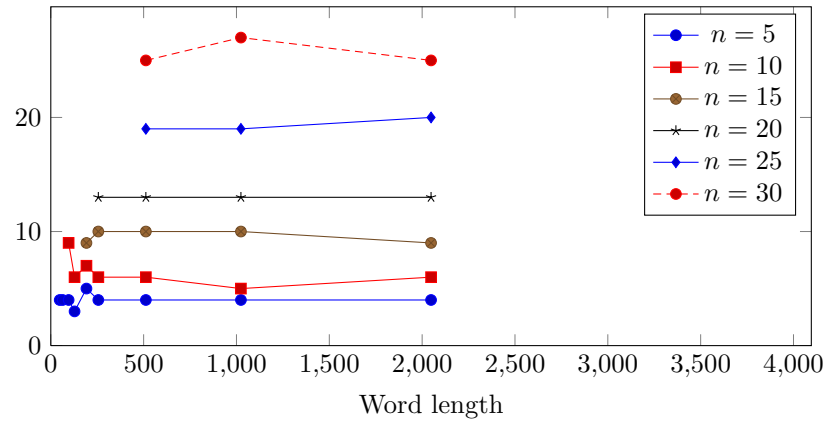
Our observations thus lead us to making the following conjecture.

Conjecture 3.1 (Stable region). *Consider the braid monoid B_n^+ for any fixed $n \in \mathbb{N}$. For $\mu_k = \text{Word}_k$, respectively URB_k , and for each i the sequences of probability measures $\lambda_{i*}(\mu_k)$ and $\rho_{i*}(\mu_k)$ on the set of simple elements converge as $k \rightarrow \infty$. Moreover, there exists a probability measure Σ on the set of simple elements and constants C and D such that*

$$\begin{aligned} \forall i > C \quad \lambda_{i*}(\mu_k) &\rightarrow \Sigma \text{ as } k \rightarrow \infty \\ \forall i > D \quad \rho_{i*}(\mu_k) &\rightarrow \Sigma \text{ as } k \rightarrow \infty \end{aligned}$$



(a) Uniformly random words



(b) Uniformly random braids

Figure 6: Start of stable region.

3.2 Bounded penetration distance

We can view a uniformly random word as the result of a random process adding one letter, chosen at random, at a time. The stable region conjecture suggests that the change to the normal form when multiplying by an atom is unlikely to penetrate into the stable region. This leads us to investigate how the normal form of a random braid changes upon multiplication by an atom.

The normal form of a word wa , where w is in normal form and a is an atom, can be calculated from the normal form of w by working through the word from the right to the left, repeatedly applying the rewriting rule $xy \rightarrow (xm)(m^{-1}y)$ where $m = \partial x \wedge y$. If at any point we have $m = \mathbf{1}$ then we can stop. If we have $xm = \Delta$ then all the following rewrites will be of the form $x\Delta \rightarrow \Delta\tau(x)$, that is, consist of an application of the Garside automorphism; we will consider this a trivial change.

Definition 3.2. For two braids x and y the penetration distance $\text{pd}(x, y)$ for the product xy is the number of simple factors at the end of the normal form of x which undergo a non-trivial change in the normal form of the product:

$$\text{pd}(x, y) = \text{cl}(x) - \max \{i \in \{0, \dots, \text{cl}(x)\} : x\Delta^{-\inf(x)} \wedge \Delta^i = xy\Delta^{-\inf(xy)} \wedge \Delta^i\}$$

Using the same samples of uniformly random words and uniformly random braids as before, we took each braid and calculated the penetration distances for its product with each generator. The mean penetration distance for each word length is shown in Figure 7. There are clear patterns here: the mean penetration distance converges as the word length increases; the value of the mean penetration distance increases with n ; and it is significantly larger for uniformly random braids than it is for uniformly random words.

Conjecture 3.3 (Bounded expected penetration distance). *Consider the braid monoid B_n^+ for any fixed $n \in \mathbb{N}$. Let μ_A be the uniform probability measure on the set of atoms. For $\mu_k = \text{Word}_k$, respectively URB_k , there exists C such that for all k ,*

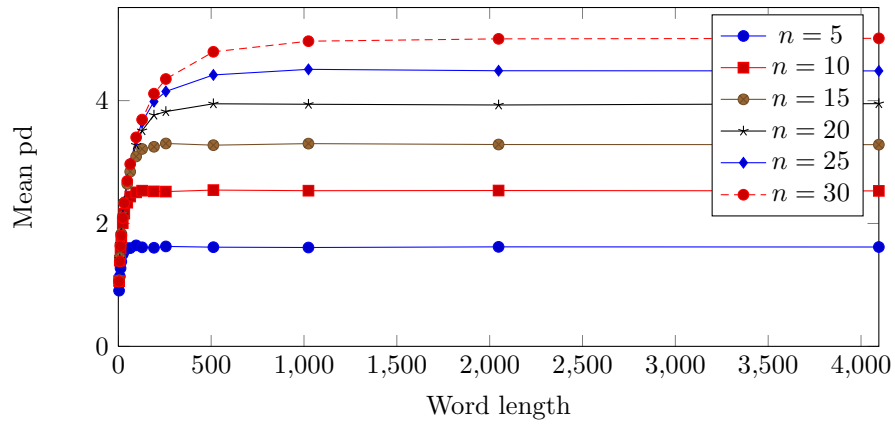
$$\mathbf{E}_{\mu_k \times \mu_A}[\text{pd}] < C$$

Corollary 3.4. *There exists an algorithm to compute the normal form of a braid that has linear expected run time.*

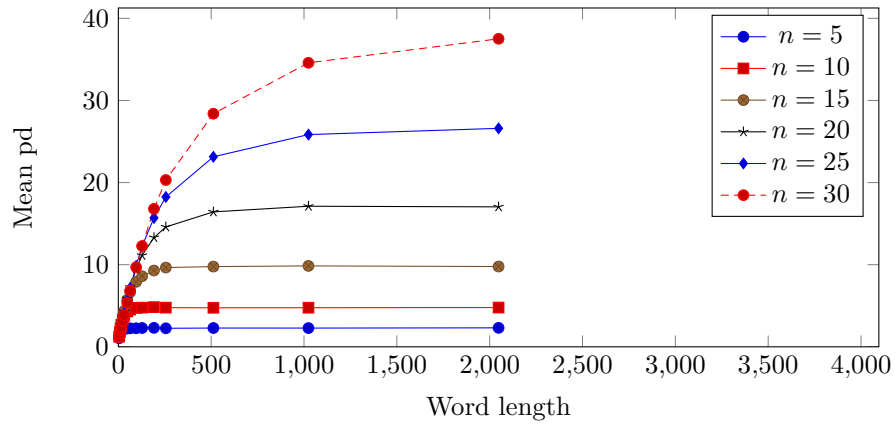
Proof. Consider Algorithm 1 for computing the left normal form of a word. The first loop is similar to the usual algorithm [ECH⁺92, Ch.9] except that: we increment a counter I each time a Δ is created, this will be the infimum of the normal form; we add a power of Δ before each simple element, these are stored modulo c the central power of Δ ; and the inner loop stops as soon as a new Δ is created. We then add an additional pass, working backwards along the word, to push all the Δ s to the front.

This algorithm has an invariant: the equality $x = \Delta^{I - \sum_i l_i} \Delta^{l_1} x_1 \Delta^{l_2} x_2 \dots \Delta^{l_k} x_k$ in B_n , where the summands in the first exponent of Δ are regarded as integers, remains true after each line has been completed.

As the l_j are elements of $\frac{\mathbb{Z}}{c\mathbb{Z}}$ the operation of “pushing” the Δ s over a simple on lines 9, 15 and 35 has bounded run time.



(a) Uniformly random words



(b) Uniformly random braids

Figure 7: Mean penetration distance.

The inner loop in line 11 pushes the change to x_i through the prefix of the word up to that point, so the contents of the loop will be executed $\text{pd}(x_1 x_2 \cdots x_{i-1}, x_i)$ times. Hence, by Conjecture 3.3 this loop is expected to take a constant amount of time. The two outer loops have at most k iterations with each iteration taking a constant expected run time, hence the whole algorithm has linear expected run time. \square

Figure 8 shows the mean penetration distance of each generator for $n = 30$ and a word length of 2048. A similar shape can be seen for the other values of n . We see that not only is the mean penetration distance longer for uniformly random braids, but also the ratio of longest to shortest is significantly larger: For uniformly random words the ratio is less than 2, but for uniformly random braids it is greater than 10.

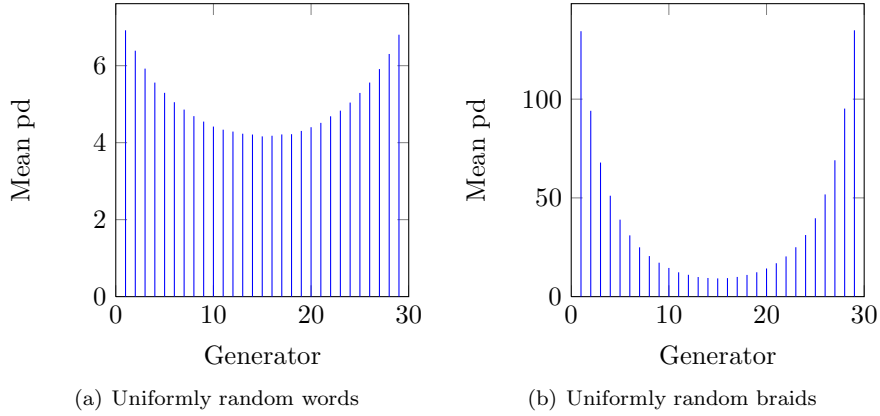


Figure 8: Mean penetration distance for each generator. $n = 30$, word length = 2048.

Figure 9 shows the distribution of penetrations distances observed in our sample for $n = 30$ and a word length of 2048.

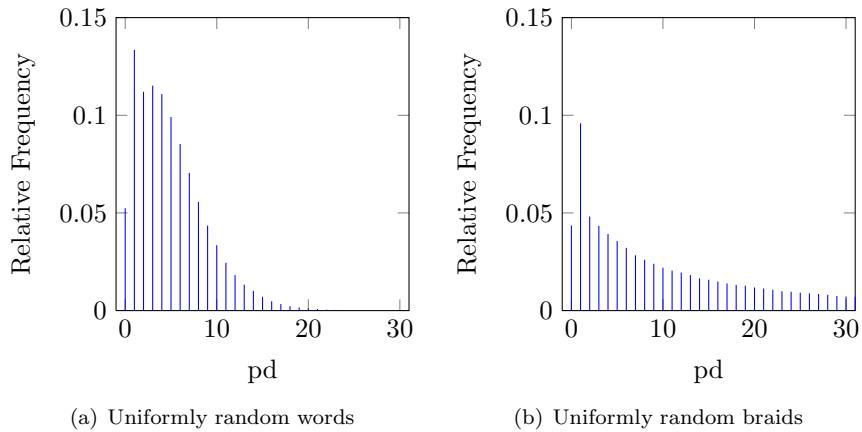


Figure 9: Distribution of penetration distances. $n = 30$, word length= 2048.

Algorithm 1 Calculate the normal form of a word x

Input: $x_1x_2 \cdots x_k \leftarrow x$ where each $x_i \in \mathcal{A}$

Output: $\Delta^I x_1x_2 \cdots x_k$

```

1:  $l_1, l_2, \dots, l_k \leftarrow 0 \in \frac{\mathbb{Z}}{c\mathbb{Z}}$ 
2:  $I \leftarrow 0 \in \mathbb{Z}$ 
3:  $i \leftarrow 1$ 
4: while  $i < k$  do
5:   if  $\partial x_i \wedge x_{i+1} \neq \mathbf{1}$  then
6:      $m \leftarrow \partial x_i \wedge x_{i+1}; \quad x_i \leftarrow x_i m; \quad x_{i+1} \leftarrow m^{-1} x_{i+1}$ 
7:      $j \leftarrow i$ 
8:     if  $j > 1$  then
9:        $x_{j-1} \leftarrow \tau^{l_j}(x_{j-1}); \quad l_{j-i} \leftarrow l_{j-1} + l_j; \quad l_j \leftarrow 0$ 
10:    end if
11:    while  $x_j \neq \Delta$  and  $j > 1$  and  $\partial x_{j-1} \wedge x_j \neq \mathbf{1}$  do
12:       $m \leftarrow \partial x_{j-1} \wedge x_j; \quad x_{j-1} \leftarrow x_{j-1} m; \quad x_j \leftarrow m^{-1} x_j$ 
13:       $j \leftarrow j - 1$ 
14:      if  $j > 1$  then
15:         $x_{j-1} \leftarrow \tau^{l_j}(x_{j-1}); \quad l_{j-i} \leftarrow l_{j-1} + l_j; \quad l_j \leftarrow 0$ 
16:      end if
17:    end while
18:    if  $x_j = \Delta$  then
19:       $l_{j+1} \leftarrow l_j + l_{j+1} + 1; \quad I \leftarrow I + 1$ 
20:      Delete  $x_j$  and  $l_j$  moving following terms forward, decreasing  $k$  by 1.
21:       $i \leftarrow i - 1$ 
22:    end if
23:    if  $x_{i+1} = \mathbf{1}$  then
24:      Delete  $x_{i+1}$  moving following terms forward, decreasing  $k$  by 1.
25:       $i \leftarrow i - 1$ 
26:    end if
27:  else
28:     $i \leftarrow i + 1$ 
29:  end if
30: end while
31: for  $j = k$  to 2 do
32:    $x_{j-1} \leftarrow \tau^{l_j}(x_{j-1}); \quad l_{j-i} \leftarrow l_{j-1} + l_j; \quad l_j \leftarrow 0$ 
33: end for
34: end for

```

3.3 Garside groups

Clearly the stable region conjecture and the bounded expected penetration distance conjecture make sense in any Garside group and for different sequences of probability measures. We will give an example of a Garside group G_1 where the penetration distance is bounded, in other words there exists a constant C such that for any element x and any atom a we have $\text{pd}(x, a) < C$. This stronger condition implies that both the bounded penetration distance conjecture and the stable region conjecture hold for G_1 . We will then go on to give a method to establish whether a variant of the bounded penetration distance conjecture holds within a given Garside group.

A small Garside group

Let G_1 be the Garside group given by the following presentation.

$$G_1 = \langle A, B \mid ABA = BB \rangle$$

This group is isomorphic (as a group) to the braid group on three strands, but the Garside structure is distinct [Deh02b]. The Garside element is BBB and there are eight simple elements. Figure 10 shows the structure of the left ordering on the simple elements. Figure 11 shows the matrix where the xy entry is 1 if $\partial x \wedge y = \mathbf{1}$ and 0 otherwise. From this matrix one can easily read off which pairs of simple element are in left normal form.

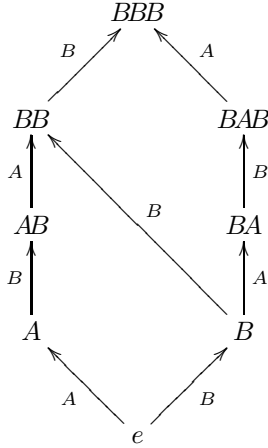


Figure 10: Hasse diagram for the left ordering on the lattice of simple elements

	A	B	AB	BA	BB	BAB
A	1	0	1	0	0	0
B	0	0	0	0	0	0
AB	0	1	0	1	0	1
BA	1	0	1	0	0	0
BB	1	0	1	0	0	0
BAB	0	1	0	1	0	1

Figure 11: The entry a, b is 1 if $\partial a \wedge b = \mathbf{1}$ and 0 otherwise.

Proposition 3.5. *For any element $x \in G_1^+$ in the positive monoid and any atom $a \in \{A, B\}$ we have*

$$\text{pd}(x, a) < 3$$

Proof. First consider the atom A and look at how the change upon multiplication by A can penetrate through possible suffixes of the left normal form of x .

If we look at sA for each simple element suffix s we see that there are three suffixes with canonical length one that have non-zero penetration distance.

s	A	B	AB	BA	BB	BAB
Normal form of sA	AA	BA	BB	$BA A$	$BB A$	Δ
$\text{pd}(s, A)$	0	1	1	0	0	1

So for a suffix s with canonical length two to have a penetration distance greater than one the last factor cannot be A , BA , or BB . We can also rule out BAB as in this case a Δ is created, which cannot affect any earlier factors. Figure 11 indicates which pairs of simple elements can be adjacent in a left normal form; using this information, we can easily produce a list of possible suffixes.

s	$AB B$	$BAB B$	$A AB$	$BA AB$	$BB AB$
N.F. of sA	$AB BA$	$BAB BA$	$AB B$	$BAB B$	ΔB
$\text{pd}(s, A)$	1	1	2	2	2

So for suffixes with canonical length three there are only two possibilities for the last two factors where the penetration distance could be greater than two: $A AB$ and $BA AB$. This gives the following list of possible suffixes.

s	$AA AB$	$BA A AB$	$BB A AB$	$AB BA AB$	$BAB BA AB$
N.F. of sA	$A AB B$	$BA AB B$	$BB AB B$	$AB BAB B$	$BAB BAB B$
$\text{pd}(s, A)$	2	2	2	2	2

Hence $\text{pd}(x, A)$ cannot be greater than two.

We will now follow the same procedure for the atom B .

If we look at each simple element we see that there are four possible suffixes with canonical length one that have non-zero penetration distance.

s	A	B	AB	BA	BB	BAB
N.F. of sB	AB	BB	$AB B$	BAB	Δ	$BAB B$
$\text{pd}(s, A)$	1	1	0	1	1	0

So for a suffix with canonical length two to have a penetration distance greater than one the last factor cannot be AB , or BAB . We can also rule out BB as a Δ is produced. This gives the following list of possible suffixes.

s	AA	$BA A$	$BB A$	$AB B$	$BAB B$	$AB BA$	$BAB BA$
N.F. of sB	$A AB$	$BA AB$	$BB AB$	ΔA	ΔBA	$AB BAB$	$BAB BAB$
$\text{pd}(s, A)$	1	1	1	2	2	1	1

All words with a penetration distance of two create a Δ so any preceding factors would not be affected. Hence $\text{pd}(x, B)$ cannot be greater than two. \square

Remark Since the Garside element Δ is central, any changes to the normal form when multiplying by an atom are limited to a fixed number of simple factors at the end of the word. This means that the normal form can be computed in a single pass with a finite state transducer (an automaton with output) which is augmented with an integer counter to count each occurrence of Δ .

Penetration sequences

In the proof of Proposition 3.5 we considered sequences of simple elements in normal form and how the change penetrated through them when we multiplied by an atom. We can formalise this idea as follows. For the rest of this section, let G^+ be a Garside monoid with Garside element Δ .

Definition 3.6. A word $(s_1, m_1)(s_2, m_2) \cdots (s_k, m_k) \in (D(\Delta) \times D(\Delta))^*$ is a penetration sequence if, for all i ,

- (3) $s_i \neq \mathbf{1}, \Delta \quad m_i \neq \mathbf{1}, \Delta$
- (4) $i > 1 \implies s_i m_i \neq \Delta$
- (5) $\partial s_i \wedge s_{i+1} = \mathbf{1}$
- (6) $m_i = \partial s_i \wedge s_{i+1} m_{i+1}$

For a penetration sequence, condition (5) ensures that $s_1 s_2 \cdots s_k$ is in normal form. If we consider how this normal form changes once we multiply by m_k then condition (6) means that m_i is the simple factor that moves out of s_{i+1} into s_i . Condition (6) also means that $s_i m_i \preceq \Delta$.

We are only interested in the canonical factors of the word and not the initial power of Δ . Also, we are only interested in the region where there is non-trivial movement between the factors. So we impose condition (3).

We only allow a Δ to be created at the very start of the sequence, as otherwise the initial terms just correspond to conjugating by Δ which we consider a trivial change. Hence condition (4).

Let PSEQ_k denote the set of all penetration sequences of length k .

For an element $x \in G^+$ and a simple element $s \in D(\Delta)$ we will say that a penetration sequence $(s_1, m_1)(s_2, m_2) \cdots (s_k, m_k)$ is a *penetration sequence for xs* if $s_1 s_2 \cdots s_k$ is a suffix of the normal form of x , and $m_k = \partial s_k \wedge s$. The penetration distance for the product xs equals the length of the longest penetration sequence for xs .

Let

$$G_{(k)}^+ := \{x \in G^+ : \text{cl}(x) = k, \inf(x) = 0\}$$

Lemma 3.7. *There exist constants $\alpha, \beta, p, q > 0$ such that*

$$|\text{PSEQ}_k| \in O(k^p \alpha^k) \quad |G_{(k)}^+| \in O(k^q \beta^k)$$

Proof. Since a word in $(D(\Delta) \times D(\Delta))^*$ is a penetration sequence if each consecutive pair of letters satisfy conditions (3)–(6), we have that $\bigcup_k \text{PSEQ}_k$ is a regular language. Similarly, $\bigcup_k G_{(k)}^+$ is also a regular language. Hence the growth functions of these languages are rational functions.

By [FS09, Theorem IV.9], if $\sum_k f_k z^k$ is a rational function with poles p_1, p_2, \dots, p_m then there exist polynomials P_1, P_2, \dots, P_m such that $f_k = \sum_i P_i(k) p_i^{-k}$, for k larger than some fixed K . Hence the results hold with α and β equal to the reciprocal of the radius of convergence of the corresponding growth function. \square

Theorem 3.8. *Let ν_k be the uniform probability measure on $G_{(k)}^+$. If the exponential growth rate of $|G_{(k)}^+|$ is greater than that of $|\text{PSEQ}_k|$, in other words $\beta > \alpha$, and $|G_{(k)}^+| \in \Omega(k^q \beta^k)$ then the expected value $\mathbf{E}_{\nu_k \times \mu_{\mathcal{A}}}[\text{pd}]$ of the penetration distance with respect to ν_k is bounded.*

Proof. If $|\text{PSEQ}_k|$ is eventually 0 then the penetration distance is bounded. So we may now assume otherwise.

If $\alpha < 1$ then for every $\epsilon > 0$ we would have that eventually $|\text{PSEQ}_k| < \epsilon$. So as $|\text{PSEQ}_k|$ takes integer values we have that $|\text{PSEQ}_k|$ is eventually 0, which is a contradiction. So we may now assume that $\alpha \geq 1$.

Let

$$X_{i,k} := \{(x, a) \in G_{(k)}^+ \times \mathcal{A} : \text{pd}(x, a) = i\}$$

Now

$$\mathbf{E}_{\nu_k \times \mu_{\mathcal{A}}}[\text{pd}] = \sum_{i=0}^k i \frac{|X_{i,k}|}{|G_{(k)}^+| \cdot |\mathcal{A}|}$$

Given $(x, a) \in X_{i,k}$, let $(s_1, m_1)(s_2, m_2) \cdots (s_l, m_l)$ be a maximal penetration sequence for xa . From the definition of $X_{i,k}$ we have that $l = i$ and, as a is an atom, $m_i = a$. The simple factors s_1, s_2, \dots, s_i will be the final i factors of the normal form of x , so $x = x_1 s_1 s_2 \cdots s_i$ for some $x_1 \in G_{(k-i)}^+$. This gives an injective map $X_{i,k} \hookrightarrow G_{(k-i)}^+ \times \text{PSEQ}_i$, therefore

$$(7) \quad |X_{i,k}| \leq |G_{(k-i)}^+| \cdot |\text{PSEQ}_i|$$

By Lemma 3.7 and the requirement that $|G_{(k)}^+| \in \Omega(k^q \beta^k)$, there exists a C and K such that for all $k > K$

$$|\text{PSEQ}_k| \leq C k^p \alpha^k \quad \frac{1}{C} k^q \beta^k \leq |G_{(k)}^+| \leq C k^q \beta^k$$

So for $k - i > K$ we have

$$(8) \quad \frac{|G_{(k-i)}^+| \cdot |\text{PSEQ}_i|}{|G_{(k)}^+|} \leq C^3 \frac{(k-i)^q \beta^{k-i} i^p \alpha^i}{k^q \beta^k} \leq C^3 i^p \left(\frac{\alpha}{\beta}\right)^i$$

For $k - i \leq K$ and $k > 2K$ we have $i > K$ and

$$(9) \quad \frac{|G_{(k-i)}^+| \cdot |\text{PSEQ}_i|}{|G_{(k)}^+|} \leq \frac{D |\text{PSEQ}_i|}{|G_{(k)}^+|} \leq C^2 D \frac{i^p \alpha^i}{k^q \beta^k} \leq C^2 D k^{p-q} \left(\frac{\alpha}{\beta}\right)^k$$

where D is the largest value of $|G_{(j)}^+|$ for $j \in \{1, 2, \dots, K\}$.

By making use of (7) and splitting the sum into two parts we have that for $k > K$,

$$\mathbf{E}_{\nu_k \times \mu_{\mathcal{A}}}[\text{pd}] \leq \underbrace{\sum_{i=0}^{k-K-1} i \frac{|G_{(k-i)}^+| \cdot |\text{PSEQ}_i|}{|G_{(k)}^+| \cdot |\mathcal{A}|}}_{S_k} + \underbrace{\sum_{i=k-K}^k i \frac{|G_{(k-i)}^+| \cdot |\text{PSEQ}_i|}{|G_{(k)}^+| \cdot |\mathcal{A}|}}_{T_k}$$

By (8)

$$S_k < \frac{C^3}{|\mathcal{A}|} \sum_{i=0}^{k-K-1} i^{p+1} \left(\frac{\alpha}{\beta} \right)^i$$

Which converges as $k \rightarrow \infty$ if $\alpha < \beta$.

By (9), if $k > 2K$ then

$$T_k < \frac{C^2 D}{|\mathcal{A}|} \sum_{i=k-K}^k i k^{p-q} \left(\frac{\alpha}{\beta} \right)^k < \frac{C^2 D K k^{p-q+1}}{|\mathcal{A}|} \left(\frac{\alpha}{\beta} \right)^k$$

Which also converges as $k \rightarrow \infty$ if $\alpha < \beta$.

Hence, if $\alpha < \beta$ then $\mathbf{E}_{\nu_k \times \mu_{\mathcal{A}}}[\text{pd}]$ is eventually bounded by a convergent sequence and so is itself bounded. \square

Calculating the exponential growth rates

Let M be the matrix with entries indexed by pairs $(s, m) \in D(\Delta) \times D(\Delta)$ such that $s, m \notin \{1, \Delta\}$ and $sm \preceq \Delta$ whose entries are as follows.

$$M_{(s_1, m_1)(s_2, m_2)} = \begin{cases} 1 & \text{if } s_2 m_2 \neq \Delta, \partial s_1 \wedge s_2 = 1, m_1 = \partial s_1 \wedge s_2 m_2 \\ 0 & \text{otherwise} \end{cases}$$

We now have

$$|\text{PSEQ}_0| = 1 \qquad |\text{PSEQ}_k| = w M^{k-1} v$$

where v is the column vector with all entries 1 and w is the row vector with all entries 1. So we can compute the initial terms of the sequence and the minimal polynomial of M gives us a recurrence relation. This allows us to compute the generating function. The exponential growth rate α is then the reciprocal of the radius of convergence of the generating function.

A similar matrix allow us to compute the generating function and exponential growth rate β for the sequence $|G_{(k)}^+|$. To verify that $|G_{(k)}^+| \in \Omega(k^q \beta^k)$ it is sufficient to check that there is a unique pole of the generating function whose absolute value is equal to the radius of convergence.

The results of applying this procedure to several different Garside groups are listed in Table 1. Here $G_1 = \langle A, B \mid ABA = A^2 \rangle$ is the group described above; $G_2 = \langle x, y, z \mid xzxy = yzx^2, yzx^2z = zxyzx, zxyzx = xzxyz \rangle$ is a Garside group described in [Pic03]; B_n is the classical Garside structure and BKL_n is the Birman-Ko-Lee Garside structure for the braid group on n strands.

Note that in all these examples $\alpha < \beta$ and the generating function for $|G_{(k)}^+|$ has a unique pole with minimal absolute value, hence all of these groups satisfy the conditions of Theorem 3.8. We can also see that, in addition to G_1 , the Garside groups B_3 and BKL_3 also have a bounded penetration distance.

Figure 12 shows a plot of α against β for these groups. A line is drawn through the BKL_4 and BKL_6 points. Although the number of points is small, the fact that all of the braid groups lie close to this line is very suggestive.

	$\sum_{k=0}^{\infty} \text{PSEQ}_k z^k$	α	$\sum_{k=0}^{\infty} G_{(k)}^+ z^k$	β
G_1	$8z^2 + 13z + 1$	0	$\frac{-z^3 - 4z - 1}{2z - 1}$	2
G_2	$\frac{-57z^3 - 102z^2 - 78z - 1}{z - 1}$	1	$\frac{-11z^3 + 13z^2 - 9z - 1}{12z^3 - 16z^2 + 13z - 1}$	11.72...
B_3	$6z + 1$	0	$\frac{-2z - 1}{2z - 1}$	2
B_4	$\frac{4z^6 - 32z^5 + 145z^4 + 178z^3 - 333z^2 + 97z + 1}{z^4 - 10z^3 + 15z^2 - 7z + 1}$	3.532...	$\frac{6z^3 - 3z^2 - 14z - 1}{6z^3 - 15z^2 + 8z - 1}$	5.449...
B_5	$\frac{280z^{36} + \dots + 1592z + 1}{4z^{34} + \dots - 68z + 1}$	12.82...	$\frac{-144z^5 + 48z^4 + 594z^3 - 307z^2 - 90z - 1}{144z^5 - 480z^4 + 498z^3 - 199z^2 + 28z - 1}$	18.71...
BKL_3	$3z + 1$	0	$\frac{-z - 1}{2z - 1}$	2
BKL_4	$\frac{8z^5 - 52z^4 + 68z^3 - 56z^2 + 23z + 1}{4z^4 - 8z^3 + 8z^2 - 5z + 1}$	3.130...	$\frac{2z^4 + 4z^3 - 5z^2 + 4z + 1}{10z^4 - 20z^3 + 19z^2 - 8z + 1}$	4.839...
BKL_5	$\frac{-2457600z^{31} + \dots + 154z + 1}{1638400z^{30} - \dots - 36z + 1}$	8.822...	$\frac{-40z^8 - 188z^7 + 444z^6 - 482z^5 + 122z^4 + 104z^3 - 73z^2 + 16z + 1}{560z^8 - 1968z^7 + 3364z^6 - 3402z^5 + 2132z^4 - 836z^3 + 197z^2 - 24z + 1}$	12.83...
BKL_6	$\frac{-66400008857169584494901775564800000000000000000000z^{178} + \dots - 956z - 1}{15164765481245908367514271744000000000000000000000z^{177} - \dots + 209z - 1}$	25.31...	$\frac{2240000z^{22} + \dots + 60z + 1}{94080000z^{22} - \dots - 70z + 1}$	35.98...

Table 1: Generating functions and exponential growth rates

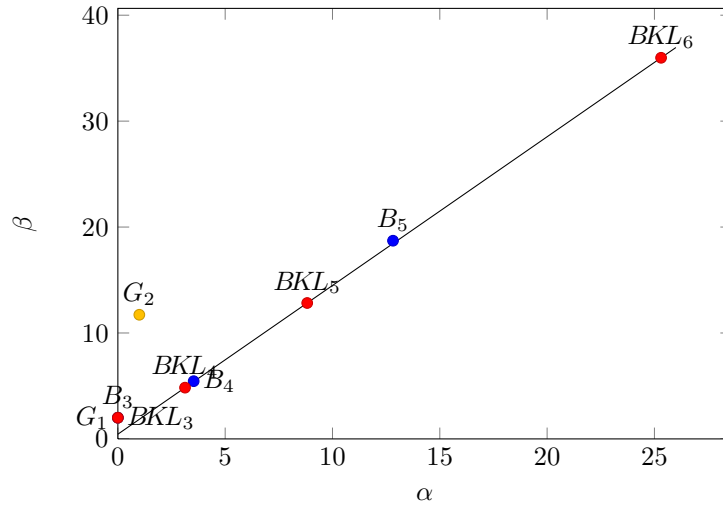


Figure 12: Scatter plot of the exponential growth rates.

References

- [AAG99] Iris Anshel, Michael Anshel, and Dorian Goldfeld. An algebraic method for public-key cryptography. *Math. Res. Lett.*, 6(3-4):287–291, 1999. MR1713130 (2000e:94034)
- [BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993). MR1484478
- [Cha95] Ruth Charney. Geodesic automation and growth functions for Artin groups of finite type. *Math. Ann.*, 301(2):307–324, 1995. MR1314589 (95k:20055)
- [Deh02a] Patrick Dehornoy. Groupes de Garside. *Ann. Sci. École Norm. Sup. (4)*, 35(2):267–306, 2002. MR1914933 (2003f:20068)
- [Deh02b] Patrick Dehornoy. Groupes de Garside. *Ann. Sci. École Norm. Sup. (4)*, 35(2):267–306, 2002. MR1914933 (2003f:20068)
- [ECH⁺92] David B. A. Epstein, James W. Cannon, Derek F. Holt, Silvio V. F. Levy, Michael S. Paterson, and William P. Thurston. *Word processing in groups*. Jones and Bartlett Publishers, Boston, MA, 1992. MR1161694 (93i:20036)
- [FS09] Philippe Flajolet and Robert Sedgewick. *Analytic combinatorics*. Cambridge University Press, Cambridge, 2009. MR2483235 (2010h:05005)
- [GGM13] Volker Gebhardt and Juan González-Meneses. Generating random braids. *J. Combin. Theory Ser. A*, 120(1):111–128, 2013. MR2971701

- [KLC⁺00] Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Junsung Kang, and Choonsik Park. New public-key cryptosystem using braid groups. In *Advances in cryptology—CRYPTO 2000 (Santa Barbara, CA)*, volume 1880 of *Lecture Notes in Comput. Sci.*, pages 166–183. Springer, Berlin, 2000. MR1850042 (2002i:94057)
- [Pic03] Matthieu Picantin. Automatic structures for torus link groups. *J. Knot Theory Ramifications*, 12(6):833–866, 2003. MR2008883 (2004i:20077)

Volker Gebhardt

School of Computing, Engineering and Mathematics
University of Western Sydney
Locked Bag 1797, Penrith NSW 2751, Australia
E-mail: `v.gebhardt@uws.edu.au`

Stephen Tawn

School of Computing, Engineering and Mathematics
University of Western Sydney
Locked Bag 1797, Penrith NSW 2751, Australia
E-mail: `stephen@tawn.co.uk`